

## A NOTE ON THE DUALS OF SKEW CONSTACYCLIC CODES

ALEXIS E. ALMENDRAS VALDEBENITO AND ANDREA LUIGI TIRONI

ABSTRACT. Let  $\mathbb{F}_q$  be a finite field with  $q$  elements and denote by  $\theta : \mathbb{F}_q \rightarrow \mathbb{F}_q$  an automorphism of  $\mathbb{F}_q$ . In this note, we deal with skew constacyclic codes, i.e. linear codes of  $\mathbb{F}_q^n$  which are invariant under the action of a semi-linear map  $T : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ , defined by  $T(a_0, \dots, a_{n-2}, a_{n-1}) := (\alpha a_{n-1}, a_0, \dots, a_{n-2})$  for some  $\alpha \in \mathbb{F}_q - \{0\}$  and  $n \geq 2$ . In particular, we study some algebraic and geometric properties of their dual codes and we give some Magma Programs as applications of the main theoretical results.

## INTRODUCTION

Let  $\mathbb{F}_q$  be a field with  $q$  elements. A linear code  $\mathcal{C}$  of length  $n$  and dimension  $k$ , called an  $[n, k]_q$ -code, is a  $k$ -dimensional subspace of  $\mathbb{F}_q^n$ . Moreover, an  $[n, k]_q$ -code  $\mathcal{C}$  with minimum Hamming distance  $d := d(\mathcal{C})$  is denoted as an  $[n, k, d]_q$ -code. A fundamental problem in Coding Theory is that of optimizing one of the parameters  $n, k, d$  for given the other two. If  $d_q(n, k)$  denotes the largest value of  $d$  for which an  $[n, k, d]_q$ -code exists, we call an  $[n, k, d_q(n, k)]_q$ -code simply an optimal code. It is well known that a large number of new linear codes achieving the best known bounds  $d_q(n, k)$ , in particular over small fields, have been constructed as cyclic, constacyclic or quasi-cyclic codes, including the corresponding ones in the non-commutative case (e.g., see [2] and [8]). For this reason, the main purpose of this note is to study some algebraic and geometric properties of skew constacyclic codes (Definition 1) and their duals, the latest ones being strongly related to the above minimum Hamming distance  $d$  which is useful in error-correcting codes and for some decoding algorithms. Finally, two lower bounds for the distance of these kind of codes are given, together with some MAGMA programs (Programs 1 to 5) as an application of the main theoretical results.

After some notions and basic remarks, in Section 1 we recall some known properties of skew constacyclic codes and as a consequence of these facts,

---

*Date:* April 14, 2016.

2010 *Mathematics Subject Classification.* Primary: 12Y05, 16Z05; Secondary: 94B05, 94B35. Key words and phrases: finite fields, constacyclic codes, dual codes, skew polynomial rings, semi-linear maps.

During the preparation of this paper in the framework of the Project Anillo ACT 1415 PIA CONICYT, the authors were partially supported by Proyecto VRID N. 214.013.039-1.OIN. Moreover, the first author was partially supported by CONICYT-PCHA/Magíster Nacional año 2013 - Folio: 221320380.

we give some geometric properties about the parity check matrices of skew constacyclic codes (Theorems 12 and 13), whose columns are composed of orbits of points in projective spaces via semi-linear maps. Furthermore, inspired by [8] and [9], we firstly generalize at the end of Section 1 a result about 1-generator QT codes to the non-commutative case (Theorem 20) and secondly, by using a factorization algorithm of A. Leroy in the commutative case, in Section 2 we give two lower bounds for the minimum Hamming distance  $d$  of skew  $\theta$ -module codes, in particular for skew constacyclic codes (Theorems 26 and 29). Finally, as an application of the above results, we write five MAGMA Programs [1] and for small fields we construct a table with some 1-generator skew QT codes (see Definition 19) which reach the known best minimum Hamming distance.

## 1. PROPERTIES OF SKEW CONSTACYCLIC CODES AND THEIR DUALS

Along all this note, we will use the following notation.

Let  $\mathbb{F}_q$  be a finite field with  $q$  elements, where  $q = p^n$  for some prime  $p$ . Define  $\mathbb{F}_q^* := \mathbb{F}_q - \{0\}$  and take  $\alpha \in \mathbb{F}_q^*$ . Let  $\theta$  be an automorphism of  $\mathbb{F}_q$  and let us recall here the definition of the main object which we will treat in this note.

**Definition 1** ([2],[4]). A linear code  $\mathcal{C} \subseteq \mathbb{F}_q^n$  is called a *skew  $(\alpha, \theta)$ -cyclic code* (simply a *skew  $\alpha$ -cyclic code*, or a  *$\theta$ -constacyclic code*) if  $\mathcal{C}$  is invariant under the semi-linear map

$$\phi_{\alpha, \theta} : (c_0, c_1, \dots, c_{n-1}) \mapsto (\alpha\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2})).$$

Moreover, for some fixed  $\theta$ , we call a linear code  $\mathcal{C} \subseteq \mathbb{F}_q^n$  a *skew constacyclic code* (or, a *skew pseudo-cyclic code*) if  $\mathcal{C}$  is a skew  $\alpha$ -cyclic code for some  $\alpha \in \mathbb{F}_q^*$ .

The above definition can be reinterpreted in an algebraic way by the following

**Proposition 2** ([4]). Let  $\alpha \in \mathbb{F}_q^*$ . A linear code  $\mathcal{C} \subseteq \mathbb{F}_q^n$  is a skew  $(\alpha, \theta)$ -cyclic code if and only if  $\mathcal{C}$  is invariant under the semi-linear map  $\mathcal{T} := \Theta \circ A$ , that is,  $(\vec{c})\mathcal{T} \in \mathcal{C}$  for all  $\vec{c} \in \mathcal{C}$ , where  $\Theta: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$  is defined by  $((c_0, \dots, c_{n-1}))\Theta := (\theta(c_0), \dots, \theta(c_{n-1}))$  and  $A$  is the  $n \times n$  matrix given by

$$A := \left( \begin{array}{c|ccc} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ \hline \alpha & 0 & \cdots & 0 \end{array} \right).$$

**Remark 3.** Let  $\mathcal{C} \subseteq \mathbb{F}_q^n$  be a skew  $(\alpha, \theta)$ -cyclic code. Then

$$\mathcal{C} \star (\Theta \circ A) \subseteq \mathcal{C},$$

where  $\mathcal{C} \star (\Theta \circ A) := \{(\vec{c})\Theta A \mid \vec{c} \in \mathcal{C}\}$ . When  $\theta = Id$ , a skew  $(\alpha, Id)$ -cyclic code is simply a constacyclic code.

From now on, we mainly show some algebraic and geometric properties for the dual code of a skew constacyclic codes.

First of all, with the purpose of giving an algebraic structure to skew  $\alpha$ -cyclic codes, write  $R := \mathbb{F}_q[x; \theta]$  and consider the following one-to-one correspondence:

$$(1) \quad \begin{aligned} \pi: \quad \mathbb{F}_q^n &\longrightarrow R/R(x^n - \alpha) \\ (a_0, a_1, \dots, a_{n-1}) &\longmapsto a_0 + a_1x + \dots + a_{n-1}x^{n-1} \end{aligned}$$

Note that  $\pi$  is an  $\mathbb{F}_q$ -linear isomorphism of vectorial spaces over  $\mathbb{F}_q$ . So, we can identify  $\mathbb{F}_q^n$  with  $R/R(x^n - \alpha)$  and any vector  $\vec{a} = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_q^n$  with the polynomial class  $\pi(\vec{a}) := \sum_{i=0}^{n-1} a_i x^i \in R/R(x^n - \alpha)$ .

Put  $m := |\langle \theta \rangle|$ . If either  $m \nmid n$  or  $\alpha \notin \mathbb{F}_q^\theta$ , we know that  $R/R(x^n - \alpha)$  is not a ring and we cannot argue about its ideals, as in the commutative case. For instance, when  $\alpha = 1$  the condition  $m \mid n$  is assumed (e.g., see [2] and [3]) and one can construct a one-to-one correspondence between skew cyclic codes and the ideals of  $R/R(x^n - 1)$ . On the other hand, the set  $R/R(x^n - \alpha)$  could be considered a left  $\mathbb{F}_q$ -module or a left  $\mathbb{F}_q[x; \theta]$ -module.

The next two results give an equivalent definition of skew constacyclic codes and some of their well-known properties.

**Theorem 4** (see, e.g., [3] and [10]). *A nonempty subset  $\mathcal{C} \subset \mathbb{F}_q^n$  is a skew  $\alpha$ -cyclic code if and only if  $\pi(\mathcal{C})$  is a left  $R$ -submodule of the left  $R$ -module  $R/R(x^n - \alpha)$ .*

**Theorem 5** (see, e.g., [2] and [4]). *Let  $\pi(\mathcal{C})$  be a left  $R$ -submodule of  $R/R(x^n - \alpha)$  with  $R := \mathbb{F}_q[x; \theta]$ , i.e.  $\mathcal{C}$  is a skew  $\alpha$ -cyclic code of  $\mathbb{F}_q^n$ . Then there exists a unique monic polynomial of minimal degree in  $R$  such that*

- (a)  $\pi(\mathcal{C}) = Rg(x)$ , i.e.  $g(x)$  is the generator polynomial of  $\pi(\mathcal{C})$ ;
- (b)  $g(x)$  is a right divisor of  $x^n - \alpha$ ;
- (c) Every  $c(x) \in \pi(\mathcal{C})$  can be written uniquely as  $c(x) = f(x)g(x) \in R/R(x^n - \alpha)$ , where  $f(x) \in R$  has degree less than or equal to  $n - \deg g(x)$ . Moreover, the dimension of  $\mathcal{C}$  is equal to  $n - \deg g(x)$ ;
- (d) If  $g(x) := \sum_{i=0}^k g_i x^i$ , then  $\mathcal{C}$  has a generator matrix  $G$  given by

$$\begin{aligned} G &= \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{n-k-1}g(x) \end{pmatrix} \\ &= \begin{pmatrix} g_0 & g_1 & \dots & g_k & 0 & 0 & \dots & 0 \\ 0 & \theta(g_0) & \theta(g_1) & \dots & \theta(g_k) & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \theta^{n-k-1}(g_0) & \theta^{n-k-1}(g_1) & \dots & \dots & \theta^{n-k-1}(g_k) \end{pmatrix}. \end{aligned}$$

For skew  $\alpha$ -cyclic codes of  $\mathbb{F}_q^n$  with  $\theta(x) := x^{p^t}$ , where  $q = p^r$  for some prime  $p$ ,  $r \in \mathbb{Z}_{\geq 2}$  and an integer  $t$  such that  $1 \leq t \leq r - 1$ , type the following Program 1 before the Programs 2 to 5:

**Program 1.**

```
p:=...; r:=...; t:=...; F<w>:=GF(p^r);
R<X>:=TwistedPolynomials(F;q:=p^t);
```

The next Program 2 constructs by the command `SD(n,a)` all the skew  $\alpha$ -cyclic codes of  $\mathbb{F}_q^n$  with  $\theta(x) := x^{p^t}$ :

**Program 2.**

```
SD:=function(n,a)
P:=[]; for i in [1..n-2] do
P:=P cat [0]; end for; T:= [-a] cat P cat [1]; f:=R!T;
V:=VectorSpace(F,n); dd:=[]; E:=[x : x in F | x ne 0];
S:=CartesianProduct(E, CartesianPower(F,n-1));
for s in S do
ll:=[s[1]] cat [p : p in s[2]];
if LeadingCoefficient(R!ll) eq 1 then
q,r:=Quotrem(f,R!ll); if r eq R![0] then
R!ll; dd := dd cat [R!ll]; end if; end if; end for;
return dd; end function;
```

**Example 6.** In  $\mathbb{F}_4^{14}$  with  $\theta(x) := x^2$ , the command `SD(14,1)` gives 603 different nontrivial right divisors of  $X^{14} - 1$ , i.e. 603 different nontrivial skew cyclic codes of  $\mathbb{F}_4^{14}$  instead of 25 different nontrivial cyclic codes of  $\mathbb{F}_4^{14}$  in the commutative case.

The following technical result will be useful to prove Theorem 8.

**Lemma 7.** *Let  $\mathcal{C} \subseteq \mathbb{F}_q^n$  be a linear code and let  $\mathcal{T}: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$  be a semi-linear map such that  $\mathcal{C} \star \mathcal{T} \subseteq \mathcal{C}$ .*

- (a) *If  $\mathcal{T}$  is invertible, then  $\mathcal{C} \star \mathcal{T} = \mathcal{C}$ . Furthermore,  $\mathcal{C} \star \mathcal{T} = \mathcal{C}$  if and only if  $\mathcal{C} \star (\mathcal{T})^{-1} = \mathcal{C}$ ;*
- (b) *if  $\mathcal{T}$  is as in Proposition 2, then  $\mathcal{C} \star \mathcal{T} = \mathcal{C} \star (\mathcal{T})^{-1} = \mathcal{C}$ ; moreover, the dual code  $\mathcal{C}^\perp$  is a linear code invariant under  $\mathcal{T}' = \Theta^{-1} \circ ({}^tA)_{\theta^{-1}}$  with  $\mathcal{C}^\perp \star \mathcal{T}' = \mathcal{C}^\perp \star (\mathcal{T}')^{-1} = \mathcal{C}^\perp$ , where  $M_{\theta^{-1}} := [\theta^{-1}(m_{ij})]$  for any matrix  $M = [m_{ij}]$ .*

*Proof.* (a) Since  $\mathcal{T}$  is invertible, the semi-linear map  $\mathcal{T}$  is injective. Hence  $|\mathcal{C} \star \mathcal{T}| = |\mathcal{C}|$ . From  $\mathcal{C} \star \mathcal{T} \subseteq \mathcal{C}$  we deduce that  $\mathcal{C} \star \mathcal{T} = \mathcal{C}$ .

(b) Note that  $\mathcal{T}$  is invertible since  $\alpha \in \mathbb{F}_q^*$ . Then we can conclude by [10, Proposition 25].  $\square$

Now, we are able to show in an easy and direct way that, similarly to the commutative case, the dual code of a skew  $\alpha$ -cyclic code is a skew  $\alpha^{-1}$ -cyclic

code. This result was first presented and proven in very different forms in [3, Theorem 8], [4, Theorem 1] and [6, Theorem 6.1].

**Theorem 8.** *Let  $\mathcal{C} \subseteq \mathbb{F}_q^n$  be a linear code and take  $\alpha \in \mathbb{F}_q^*$ . Then  $\mathcal{C}$  is a skew  $\alpha$ -cyclic code if and only if its dual code  $\mathcal{C}^\perp$  is a skew  $\alpha^{-1}$ -cyclic code.*

*Proof.* Suppose that  $\mathcal{C}$  is a skew  $\alpha$ -cyclic code invariant under the semi-linear map  $\Theta \circ A$ , that is,  $\mathcal{C} \star (\Theta \circ A) \subseteq \mathcal{C}$ . By Lemma 7(b), we have

$$\mathcal{C}^\perp \star (\Theta^{-1} \circ ({}^tA)_{\theta^{-1}}) = \mathcal{C}^\perp.$$

Since  $\Theta \circ M_\theta = M \circ \Theta$  for any matrix  $M$ , by Lemma 7(a) we get

$$\begin{aligned} \mathcal{C}^\perp \star (\Theta^{-1} \circ ({}^tA)_{\theta^{-1}}) = \mathcal{C}^\perp &\iff \mathcal{C}^\perp \star (\Theta^{-1} \circ ({}^tA)_{\theta^{-1}})^{-1} = \mathcal{C}^\perp \\ &\iff \mathcal{C}^\perp \star ((({}^tA)^{-1})_{\theta^{-1}} \circ \Theta) = \mathcal{C}^\perp \\ &\iff \mathcal{C}^\perp \star (\Theta \circ ({}^tA)^{-1}) = \mathcal{C}^\perp, \end{aligned}$$

where

$$({}^tA)^{-1} = \left( \begin{array}{c|ccc} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ \hline \alpha^{-1} & 0 & \cdots & 0 \end{array} \right).$$

Thus we can conclude that  $\mathcal{C}^\perp$  is a skew  $\alpha^{-1}$ -cyclic code.

Finally, having in mind that  $(\mathcal{C}^\perp)^\perp = \mathcal{C}$ , the converse of the statement can be immediately obtained.  $\square$

**Corollary 9** (see, Proposition 13 of [3], or Proposition 1 of [5]). *Let  $\mathcal{C} \subseteq \mathbb{F}_q^n$  be a skew  $\alpha$ -cyclic code. If  $\mathcal{C} = \mathcal{C}^\perp$ , then  $n$  is even and  $\alpha = \pm 1$ .*

*Proof.* First of all, observe that  $n = \dim \mathcal{C} + \dim \mathcal{C}^\perp = 2 \dim \mathcal{C}$ . Finally, let  $g(x)$  be the generator polynomial of  $\mathcal{C}$ . By Theorem 8 we have

$$X^n - \alpha = h_1(x)g(x) \quad \text{and} \quad X^n - \alpha^{-1} = h_2(x)g(x),$$

for some  $h_1(x), h_2(x) \in R$ . So we get  $\deg[(h_1(x) - h_2(x))g(x)] = 0$  and since  $\deg g(x) > 0$ , we conclude that  $h_2(x) = h_1(x)$  and this shows that  $\alpha = \alpha^{-1}$ , i.e.  $\alpha^2 = 1$ .  $\square$

With the next result one can write directly the generator polynomial of the dual code of any skew constacyclic code.

**Proposition 10** (see, Theorem 8 of [3], or Theorem 6.1 of [6]). *Let  $\mathcal{C} \subseteq \mathbb{F}_q^n$  be a skew  $\alpha$ -cyclic code generated by the polynomial  $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$ . Then the dual code  $\mathcal{C}^\perp$  is generated by*

$$h(x) := \theta^k(\bar{h}_0^{-1}) \left[ \sum_{i=0}^k \theta^i(\bar{h}_{k-i}) x^i \right],$$

where  $\bar{h}(x) := \bar{h}_0 + \bar{h}_1x + \cdots + \bar{h}_kx^k$  is such that  $x^n - \theta^{-k}(\alpha) = g(x)\bar{h}(x)$ .

*Proof.* Since  $\mathcal{C}$  is a skew  $\alpha$ -cyclic code, by Theorem 8 we know that the dual code  $\mathcal{C}^\perp$  is a skew  $\alpha^{-1}$ -cyclic code. Thus from Theorem 5 it follows that there exists a unique monic polynomial  $h(x)$  of minimal degree in  $R := \mathbb{F}_q[x; \theta]$  such that  $\mathcal{C}^\perp = Rh(x)$ . Therefore by [3, Theorem 8] we deduce that there exist  $\tilde{h}(x) \in R$  and  $c \in \mathbb{F}_q^*$  such that

$$X^n - c = g(x)\tilde{h}(x)$$

and  $h(x) = \theta^k(\tilde{h}_0^{-1})g^\perp(x)$ , where  $g^\perp(x) := \sum_{i=0}^k \theta^i(\tilde{h}_{k-i})x^i$  and  $\tilde{h}(x) = \tilde{h}_0 + \tilde{h}_1x + \cdots + \tilde{h}_kx^k$ . Since  $g(x) \in R$  is monic and  $X^n - \alpha = t(x)g(x)$  for some monic  $t(x) \in R$ , by [4, Lemma 2] we obtain that

$$X^n - \theta^{-k}(\alpha) = g(x)s(x)$$

for some  $s(x) \in R$ . Hence  $c - \theta^{-k}(\alpha) = g(x)(s(x) - \tilde{h}(x))$  and since  $\deg g(x) \geq 1$ , we conclude that  $c = \theta^{-k}(\alpha)$ .  $\square$

The following MAGMA Program 3 defines a function `DualCode(n,a,g)` which gives all the main informations about the dual code of a skew  $\alpha$ -cyclic codes of length  $n$  with generator polynomial  $g$  :

### Program 3.

```
DualCode:=function(n,a,g)
k:=n-Degree(R!g); C:=a^(p^(k*(r-t))); P:=[0];
for i in [1..n-2] do
P:=P cat [0]; end for;
T:= [-C] cat P cat [1]; f:=R!T; g1:=R!g; E:=[x : x in F | x ne 0];
S:=CartesianProduct(E, CartesianPower(F, n-Degree(g1)));
for ss in S do
ll:=[ss[1]] cat [p : p in ss[2]];
if g1*R!ll eq f then
h:=R!ll; end if; end for;
d:=Degree(h); h1:=Matrix(F, 1, d+1, [Eltseq(h)[i] : i in {1..d+1}]);
h2:=ReverseColumns(h1);
h3:=Matrix(F, 1, d+1, [h2[1][i]^(p^t)^(i-1) : i in {1..d+1}]);
h4:=(1/h3[1][d+1])*h3; h5:=R!h4[1][i] : i in {1..d+1}];
k:=Degree(f)-Degree(h5); V:=VectorSpace(F, n);
H:=Matrix(F, k, n, [V!(HorizontalJoin(Matrix(1, j+Degree(h5)+1,
Eltseq((R![0,1])^j*h5)), ZeroMatrix(F, 1, n-j-Degree(h5)-1)))) :
j in {0..k-1}]); k2:=Degree(f)-Degree(g1);
G:=Matrix(F, k2, n, [V!(HorizontalJoin(Matrix(1, j+Degree(g1)+1,
Eltseq((R![0,1])^j*g1)), ZeroMatrix(F, 1, n-j-Degree(g1)-1)))) :
j in {0..k2-1}]); L:=LinearCode(G); LD:=LinearCode(H);
print "===== "; print " ";
print "Code Skew", a, "-cyclic of type: ", n, k2, MinimumWeight(L);
print " "; print "Polynomial generator: "; print g1; print " ";
print "Generator Matrix: "; print G; print " ";
```

```

print "-----"; print " ";
print "Dual Code Skew", 1/a, "-cyclic of type: ", n, k,
MinimumWeight(LD); print " "; print "Check Polynomial:";
print h5; print " "; print "Parity Check Matrix:"; print H;
print " "; print G*Transpose(H); Q:= [0];
print "===== ";
for j in [1..n-2] do
Q:=Q cat [0]; end for;
U:= [-a^-1] cat P cat [1]; Z:=R!U; Z; h5;
Quotrem(R!Z,R!h5); return "end";
end function;

```

**Example 11.** Consider the finite field  $\mathbb{F}_4 = \{0, 1, w, w^2\}$ , where  $w^2 + w + 1 = 0$ , and the Frobenius automorphism  $\theta : \mathbb{F}_4 \rightarrow \mathbb{F}_4$  defined by  $\theta(x) = x^2$ . Let  $\mathcal{C}$  be the skew  $w$ -cyclic  $[8, 2, 4]_4$ -code generate by the polynomial  $x^6 + wx^4 + w^2x^2 + 1$  (command `SD(8,w)` in Program 1) with generator matrix

$$\begin{pmatrix} 1 & 0 & w^2 & 0 & w & 0 & 1 & 0 \\ 0 & 1 & 0 & w & 0 & w^2 & 0 & 1 \end{pmatrix}.$$

By the command `DualCode(8,w,[1,0,w^2,0,w,0,1])` in Program 2 we see that the dual code  $\mathcal{C}^\perp$  is the skew  $w^2$ -cyclic  $[8, 6, 2]_4$ -code ( $w^2 = w^{-1}$ ) generated by the polynomial  $x^2 + w^2$  and with generator matrix

$$\begin{pmatrix} 1 & 0 & w & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & w^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & w & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & w^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & w & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & w^2 \end{pmatrix}.$$

The following two results show a geometric property of the dual codes of skew constacyclic codes. More precisely, we will see that the columns of a parity check matrix of a skew constacyclic code can be considered as points in a projective space which are particular orbits under the action of the semi-linear map associated to the code. Therefore, in line with [7], in the non-commutative case we obtain the following two results.

**Theorem 12.** *Let  $\mathcal{C}$  be a linear  $[n, n - k]$ -code over  $\mathbb{F}_q$ . Then  $\mathcal{C}$  is a skew  $\alpha$ -cyclic code if and only if  $\mathcal{C}$  has a parity check matrix of the form*

$$[P_t, (P\tau)_t, (P\tau^2)_t, \dots, (P\tau^{n-1})_t]$$

such that  $P\tau^n = \alpha P$ , where  $P \in \mathbb{F}_q^k$ ,  $\tau = \Theta \circ T$  and  $T \in GL(k, q)$ .

*Proof.* “ $\Rightarrow$ ” Let  $\mathcal{C}$  be a skew  $\alpha$ -cyclic  $[n, n - k]$ -code over  $\mathbb{F}_q$  with a parity check matrix  $H = [(P_1)_t, (P_2)_t, \dots, (P_n)_t]$ , where  $(P_i) \in \mathbb{F}_q^k$ . Then by Theorem 8 we see that  $H' = [\alpha^{-1}\Theta((P_n)_t), \Theta((P_1)_t), \Theta((P_2)_t), \dots, \Theta((P_{n-1})_t)]$  is

also a parity check matrix for  $\mathcal{C}$ . Thus there is a matrix  $T_t \in GL(k, q)$  such that  $H = T_t \cdot H'$ . This gives

$$\begin{aligned} (P_1)_t &= T_t(\alpha^{-1}\Theta((P_n)_t)) = (\alpha^{-1}(P_n)\Theta \circ T)_t \\ (P_2)_t &= T_t\Theta((P_1)_t) = ((P_1)\Theta \circ T)_t \\ (P_3)_t &= T_t\Theta((P_2)_t) = ((P_2)\Theta \circ T)_t = ((P_1)(\Theta \circ T)^2)_t \\ &\vdots \\ (P_n)_t &= T_t\Theta((P_n)_t) = ((P_{n-1})\Theta \circ T)_t = ((P_1)(\Theta \circ T)^{n-1})_t \end{aligned}$$

Furthermore, we have

$$P_1 = \alpha^{-1}(P_n)(\Theta \circ T) \Rightarrow P_1 = \alpha^{-1}(P_1)(\Theta \circ T)^n \Rightarrow \alpha P_1 = P_1(\Theta \circ T)^n$$

So, by putting  $\tau := \Theta \circ T$  and  $P := P_1$ , we obtain that

$$H = [P_t, (P\tau)_t, (P\tau^2)_t, \dots, (P\tau^{n-1})_t]$$

with  $P\tau^n = \alpha P$ .

“ $\Leftarrow$ ” Let  $\mathcal{C}$  be a code with parity check matrix

$$H = [P_t, (P\tau)_t, (P\tau^2)_t, \dots, (P\tau^{n-1})_t]$$

with  $P \in \mathbb{F}_q^k$ ,  $\tau = \Theta \circ T$  and  $T \in GL(k, q)$  such that  $P\tau^n = \alpha P$ . Then, for any  $\vec{c} = (c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$  we have  $\vec{c}H_t = \vec{0}$ . This implies

$$\begin{aligned} \sum_{i=0}^{n-1} c_i(P\tau^i) &= \vec{0} \implies \left( \sum_{i=0}^{n-1} c_i(P\tau^i) \right) \tau = (\vec{0})\tau \\ &\implies \sum_{i=0}^{n-2} \theta(c_i)(P\tau^{i+1}) + \theta(c_{n-1})(P\tau^n) = \vec{0} \\ &\implies \sum_{i=0}^{n-2} \theta(c_i)(P\tau^{i+1}) + \theta(c_{n-1})(\alpha P) = \vec{0} \\ &\implies (\alpha\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2}))H_t = \vec{0}, \end{aligned}$$

i.e.  $(\alpha\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2})) \in \mathcal{C}$  and  $\mathcal{C}$  is a skew  $\alpha$ -cyclic code.  $\square$

**Theorem 13.** Let  $g(x) = \sum_{i=0}^k a_i x^i$  with  $a_k = 1$  be a skew polynomial of degree  $k$  in  $\mathbb{F}_q[x; \theta]$  that divides on the right  $x^n - \alpha$ , where  $\alpha \in \mathbb{F}_q^*$ . Then  $\mathcal{C} \subset \mathbb{F}_q^n$  is a skew  $\alpha$ -cyclic  $[n, n-k]$ -code over  $\mathbb{F}_q$  with generator polynomial  $g(x)$  if and only if  $\mathcal{C}$  is a code with parity check matrix

$$[P_t, (P\tau)_t, (P\tau^2)_t, \dots, (P\tau^{n-1})_t],$$



where  $P = (1, 0, \dots, 0)$ ,  $\tau = \Theta \circ T_g$  and  $T_g$  is the companion matrix of  $g(x)$ , i.e.

$$T_g = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{k-1} \end{pmatrix}.$$

*Proof.* Consider the following linear map

$$(2) \quad \begin{aligned} \pi: \quad \mathbb{F}_q^k &\longrightarrow R/Rg \\ (c_0, c_1, \dots, c_{k-1}) &\longmapsto c_0 + c_1x + \cdots c_{k-1}x^{k-1} \end{aligned}$$

with  $R = \mathbb{F}_q[x; \theta]$ . Then, we can see that  $\pi(P\tau^i) = x^i$  with  $P = (1, 0, \dots, 0)$ , for all  $i \in \mathbb{Z}_{\geq 0}$ . Thus, we have

$$\begin{aligned} \pi(a_0P + \cdots + a_{k-1}P\tau^{k-1} + P\tau^k) &= \pi(a_0P) + \cdots + \pi(a_{k-1}P\tau^{k-1}) + \pi(P\tau^k) \\ &= a_0\pi(P) + \cdots + a_{k-1}\pi(P\tau^{k-1}) + \pi(P\tau^k) \\ &= a_0(1) + a_1(x) + \cdots + a_{k-1}(x^{k-1}) + (x^k) \\ &= g(x) = 0 \in R/Rg(x), \end{aligned}$$

i.e.  $a_0P + a_1P\tau + \cdots + a_{k-1}P\tau^{k-1} + P\tau^k = (0, \dots, 0) = \vec{0}$ . Furthermore, as  $g(x)$  is a right divisor of  $x^n - \alpha$ , we have

$$\pi(P\tau^n - \alpha P) = \pi(P\tau^n) - \alpha\pi(P) = x^n - \alpha = 0 \in R/Rg(x),$$

and this implies that  $P\tau^n - \alpha P = (0, 0, \dots, 0)$ , that is,  $P\tau^n = \alpha P$ .

Take  $H = [(P_0)_t, (P_1)_t, \dots, (P_{n-1})_t]$ ,  $P_i = P\tau^i$ ,  $P_0 = P = (1, 0, \dots, 0)$  and  $\tau = \Theta \circ T_g$ .

“ $\Leftarrow$ ” Note that  $\vec{g} = (a_0, a_1, \dots, a_{k-1}, 1, 0, \dots, 0) \in \mathbb{F}_q^n$  is an element of  $\mathcal{C}$ , since  $\vec{g}H_t = \vec{0}$ . Furthermore, we get  $\vec{g}\tau^i H_t = \vec{0}$  for every  $i = 0, \dots, n-k-1$ , i.e.  $\{\vec{g}, \vec{g}\tau, \dots, \vec{g}\tau^{n-k-1}\}$  are  $n-k$  linear independent elements of  $\mathcal{C}$ . Thus  $\mathcal{C}$  has a parity check matrix  $G$  given by

$$(3) \quad \begin{pmatrix} a_0 & a_1 & \cdots & a_{k-1} & 1 & 0 & 0 & \cdots & 0 \\ 0 & \theta(a_0) & \theta(a_1) & \cdots & \theta(a_{k-1}) & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \theta^{n-k-1}(a_0) & \theta^{n-k-1}(a_1) & \cdots & \cdots & \theta^{n-k-1}(a_{k-1}) & 1 \end{pmatrix}.$$

As  $P\tau^n = \alpha P$ , by Theorem 12 we see that  $H$  is a parity check matrix of a skew  $\alpha$ -cyclic  $[n, n-k]$ -code. Finally, since  $g(x)$  is a monic polynomial which corresponds to the vector  $\vec{g} \in \mathcal{C}$ , we conclude that  $\mathcal{C}$  is a skew  $\alpha$ -cyclic  $[n, n-k]$ -code over  $\mathbb{F}_q$  with generator polynomial  $g(x)$ .

“ $\Rightarrow$ ” Let  $\mathcal{C}$  be a skew  $\alpha$ -cyclic  $[n, n-k]$ -code over  $\mathbb{F}_q$  with generator polynomial  $g(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} + x^k$ . Then the generator matrix of

$\mathcal{C}$  in the canonical form is as in (3). Let us show now that  $H$  is the parity check matrix of  $\mathcal{C}$ . From  $a_0P + a_1P\tau + \dots + a_{k-1}P\tau^{k-1} + P\tau^k = \vec{0}$ , it follows that

$$\begin{aligned} (a_0P + \dots + P\tau^k)\tau &= \vec{0} \Leftrightarrow (\theta(a_0)P\tau + \theta(a_1)P\tau^2 + \dots + P\tau^{k+1}) = \vec{0} \\ (a_0P + \dots + P\tau^k)\tau^2 &= \vec{0} \Leftrightarrow (\theta^2(a_0)P\tau^2 + \theta^2(a_1)P\tau^3 + \dots + P\tau^{k+2}) = \vec{0} \\ &\vdots \\ (a_0P + \dots + P\tau^k)\tau^{n-k-1} &= \vec{0} \Leftrightarrow (\theta^{n-k-1}(a_0)P\tau^{n-k-1} + \dots + P\tau^{n-1}) = \vec{0}. \end{aligned}$$

This implies that  $GH_t = O$ , i.e.  $HG_t = O$  and  $H$  is a parity check matrix of  $\mathcal{C}$ .  $\square$

As an application of Theorem 13, the following MAGMA Program 4 defines the function  $\text{PCM}(\mathbf{n}, \mathbf{g})$  which gives the parity check matrix in standard form of a skew a-cyclic codes in  $\mathbb{F}_q^n$  with generator polynomial  $g$  :

**Program 4.**

```
PCM:=function(n,g)
V:=VectorSpace(F,n); g1:=R!g;
if Degree(g1) ge 1 then
d:=Degree(g1); CM:=VerticalJoin(HorizontalJoin(
ZeroMatrix(F,d-1,1), ScalarMatrix(F,d-1,1)), Matrix(F,1,d,
[-Eltseq(g1)[k]: k in {1..d}])); P:=HorizontalJoin(
Matrix(F,1,1,[1]), ZeroMatrix(F,1,d-1)); TT:=R![0,1];
PP:=P; PCM1:=P; PCM2:=P; for m in {1..n-1} do
PCM1:=Matrix(F,1,d,[SpecialEvaluate(TT,PCM1[1][i]):
i in {1..d}])*CM; PCM2:=VerticalJoin(PCM2,PCM1);
end for; PCM3:=Transpose(PCM2); print
"====="; print " ";
print "Polynomial generator:"; print g1; print " ";
print "Companion Matrix:"; print CM; print " ";
print "Parity Check Matrix:"; print PCM3; print " ";
print "=====";
end if; return "end"; end function;
```

**Example 14.** Consider the finite field  $\mathbb{F}_4 = \{0, 1, w, w^2\}$ , where  $w^2 + w + 1 = 0$ , and the Frobenius automorphism  $\theta$  defined by  $\theta(x) = x^2$  for any  $x \in \mathbb{F}_4$ . The skew  $w$ -cyclic  $[7, 3]_4$ -code generate by the polynomial  $g(x) = x^4 + x^2 + w^2x + 1$  has a generator matrix

$$G := \begin{pmatrix} 1 & w^2 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & w & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & w^2 & 1 & 0 & 1 \end{pmatrix}.$$

By the command  $\text{PCM}(7, [1, w^2, 1, 0, 1])$  in Program 4, we obtain that its parity check matrix is  $H := [P_t, (P\tau)_t, (P\tau^2)_t, \dots, (P\tau^6)_t]$ , where  $P =$

$(1, 0, 0, 0)$ ,  $\tau = \Theta \circ T_g$  and  $T_g$  is the companion matrix of  $g(x)$ :

$$T_g = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & w^2 & 1 & 0 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & w^2 & 1 & w^2 \\ 0 & 0 & 1 & 0 & 1 & w & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & w^2 \end{pmatrix}.$$

**Definition 15** (see [7]). A linear code  $\mathcal{C} \subseteq \mathbb{F}_q^n$  with parity check matrix of the form

$$[P_t, (P\tau)_t, (P\tau^2)_t, \dots, (P\tau^{n-1})_t],$$

with  $P \in \mathbb{F}_q^k$ ,  $\tau = \Theta \circ T$  y  $T \in GL(k, q)$  is called a code  $\mathcal{C}$  defined by  $(\tau, P, n)$ . Furthermore, one can define also the following set

$$\Gamma_k^\alpha := \{(\tau, P, n) \mid \exists \text{ a skew } \alpha\text{-cyclic } [n, n-k]_q\text{-code defined by } (\tau, P, n)\}.$$

**Proposition 16.** Let  $\mathcal{C}_i$  be the code defined by  $(\tau_i, P_i, n) \in \Gamma_k^\alpha$  for  $i = 1, 2$ . Then,  $\mathcal{C}_1 = \mathcal{C}_2$  if and only if there exists a matrix  $S \in GL(k, q)$  such that  $\tau_1 = S \cdot \tau_2 \cdot S^{-1}$  and  $P_1 S = P_2$ .

*Proof.* “ $\Rightarrow$ ” Since  $\mathcal{C}_1 = \mathcal{C}_2$ , there exists a matrix  $S \in GL(k, q)$  such that

$$\begin{aligned} S_t[(P_1)_t, (P_1\tau_1)_t, \dots, (P_1\tau_1^{n-1})_t] &= [(P_1S)_t, (P_1\tau_1S)_t, \dots, (P_1\tau_1^{n-1}S)_t] \\ &= [(P_2)_t, (P_2\tau_2)_t, (P_2\tau_2^2)_t, \dots, (P_2\tau_2^{n-1})_t] \end{aligned}$$

From the first columns we deduce that  $P_1S = P_2$ , that is,  $P_2S^{-1} = P_1$ . Furthermore,  $P_2\tau_2^i = P_1\tau_1^iS = (P_2S^{-1})\tau_1^iS = P_2(S^{-1}\tau_1S)^i$ , with  $i = 1, \dots, n-1$ .

Thus  $\{P_2, P_2\tau_2, \dots, P_2\tau_2^{k-1}\}$  are linearly independent vectors of  $\mathbb{F}_q^n$  and a vector  $\vec{v} \in \mathbb{F}_q^n$  can be written as  $\vec{v} = \sum_{i=0}^{k-1} \lambda_{ij} (P_2\tau_2^i)$ . So we have

$$\begin{aligned} \vec{v}\tau_2 &= \sum_{i=0}^{k-1} \lambda_{ij} (P_2\tau_2^i) \tau_2, & \vec{v}(S^{-1}\tau_1S) &= \sum_{i=0}^{k-1} \lambda_{ij} (P_2\tau_2^i) (S^{-1}\tau_1S) \\ &= \sum_{i=0}^{k-1} \lambda_{ij} (P_2\tau_2^{i+1}) & &= \sum_{i=0}^{k-1} \lambda_{ij} (P_2(S^{-1}\tau_1S)^i) (S^{-1}\tau_1S) \\ &= \sum_{i=0}^{k-1} \lambda_{ij} (P_2(S^{-1}\tau_1S)^{i+1}) & &= \sum_{i=0}^{k-1} \lambda_{ij} (P_2(S^{-1}\tau_1S)^{i+1}) \end{aligned}$$

Since  $\vec{e}_j\tau_2 = \vec{e}_jS^{-1}\tau_1S$  for any canonical vector  $\vec{e}_j$  with  $j = 1, \dots, k$ , we conclude that  $S^{-1}\tau_1S = \tau_2$ .

“ $\Leftarrow$ ” Since there is a matrix  $S \in GL(k, q)$  such that  $\tau_2 = S^{-1} \cdot \tau_1 \cdot S$  y  $P_1 = P_2S^{-1}$ , we see that

$$\begin{aligned} [(P_2)_t, (P_2\tau_2)_t, \dots, (P_2\tau_2^{n-1})_t] &= [(P_1S)_t, (P_1\tau_1S)_t, (P_1\tau_1^2S)_t, \dots, (P_1\tau_1^{n-1}S)_t] \\ &= S_t[(P_1)_t, (P_1\tau_1)_t, (P_1\tau_1^2)_t, \dots, (P_1\tau_1^{n-1})_t]. \end{aligned}$$

By Theorem 12, the matrices defined by  $(\tau_1, P_1, n)$  and  $(\tau_2, P_2, n)$  are parity check matrices of skew  $\alpha$ -cyclic codes which differ by an invertible matrix, i.e. they correspond to the same code. Hence  $\mathcal{C}_1 = \mathcal{C}_2$ .  $\square$

**Remark 17.** Unlike the commutative case (see [7, Theorem 4]), when  $\theta \neq id$  we have to consider the minimal polynomial  $m_\tau$  of a semi-linear map  $\tau$  (see [11, Proposition 3.2]) instead of the characteristic polynomial. On the other hand, a minimal polynomial may be associated with two different codes. In fact, if  $\mathcal{C}_1 = \mathcal{C}_2$  then  $m_{\tau_1} = m_{\tau_2}$ , but the reverse is not true in general, as the following example shows.

**Example 18.** Consider  $R := \mathbb{F}_4[x; \theta]$ ,  $g_1 = 1 + wx + x^2 + x^3$  and  $g_2 = 1 + w^2x + x^2 + x^3$  in  $R$ , where  $\theta$  is the Frobenius automorphism. Let  $\mathcal{C}_i := Rg_i$  be a skew 1-cyclic  $[14, 11]_4$ -codes for  $i = 1, 2$ . Since  $g_1(x) \neq g_2(x)$  in  $R/R(x^{14} - 1)$ , we have  $\mathcal{C}_1 \neq \mathcal{C}_2$ . On the other hand, we get

$$\tau_1 = \Theta \circ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha & 1 \end{pmatrix}, \quad \tau_2 = \Theta \circ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha^2 & 1 \end{pmatrix}$$

with minimal polynomials  $m_{\tau_1}(x) = m_{B_1}(x^2) = x^6 + x^2 + 1$  and  $m_{\tau_2}(x) = m_{B_2}(x^2) = x^6 + x^2 + 1$  respectively (e.g., see [11]), where

$$\begin{aligned} B_1 &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha & 1 \end{pmatrix}_\theta \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha & 1 \end{pmatrix}, & B_2 &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha^2 & 1 \end{pmatrix}_\theta \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha^2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha^2 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha & 1 \end{pmatrix} & &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha^2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & 1 \\ 1 & \alpha & 1 \\ 1 & \alpha^2 & \alpha \end{pmatrix} & &= \begin{pmatrix} 0 & 0 & 1 \\ 1 & \alpha^2 & 1 \\ 1 & \alpha & \alpha^2 \end{pmatrix}, \\ m_{B_1}(t) &= \det \begin{pmatrix} -t & 0 & 1 \\ 1 & \alpha - t & 1 \\ 1 & \alpha^2 & \alpha - t \end{pmatrix}, & m_{B_2}(t) &= \det \begin{pmatrix} -t & 0 & 1 \\ 1 & \alpha^2 - t & 1 \\ 1 & \alpha & \alpha^2 - t \end{pmatrix} \\ &= t^3 + t + 1 & &= t^3 + t + 1. \end{aligned}$$

This shows that there exist two different linear codes  $\mathcal{C}_i := Rg_i$ ,  $i = 1, 2$ , with the same associated minimal polynomial  $m_{\tau_i}(x)$ .

Finally, let us consider also 1-generator skew quasi-twisted codes which can be easily defined from the notion of 1-generator QT codes (see [8, §1]).

So, similarly to [8], we give first the following

**Definition 19.** Take  $\alpha \in \mathbb{F}_q^*$  and let  $\theta$  be an automorphism of  $\mathbb{F}_q$ . Denote by  $R = \mathbb{F}_q[x; \theta]/(x^N - \alpha)$  the polynomial ring  $\mathbb{F}_q[x; \theta]$  over  $\mathbb{F}_q$  module  $x^N - \alpha$ . For

$$\mathbf{g} = (g_1(x), g_2(x), \dots, g_m(x)) \in R^N,$$

the set

$$\mathbf{C}_g = \{(r(x)g_1(x), r(x)g_2(x), \dots, r(x)g_m(x)) \mid r(x) \in R\}$$

is called the 1-generator Skew Quasi-Twisted (SQT) code with generator  $\mathbf{g}$ . Moreover, if  $\alpha = 1$  then  $\mathbf{C}_g$  is called the 1-generator Skew Quasi-Cyclic (SQC) code with generator  $\mathbf{g}$ .

From Theorem 13 we know that an  $[n, n - k]$ -code over  $\mathbb{F}_q$  is a skew  $\alpha$ -cyclic code with generator polynomial  $g(x) = \sum_{i=0}^k a_i x^i$  with  $a_k = 1$  if and only if  $\mathcal{C}$  is a linear code with parity check matrix

$$[g^n] := [P_t, (P\tau)_t, (P\tau^2)_t, \dots, (P\tau^{n-1})_t],$$

where  $P = (1, 0, \dots, 0)$ ,  $\tau = \Theta \circ T_g$  and  $T_g$  is the companion matrix of  $g(x)$ . Now, let  $\mathcal{T}$  be the projective map of  $\mathbb{P}^{k-1}(\mathbb{F}_q)$  defined by  $\tau$ . We can say that  $\mathcal{T}$  is defined by  $g(x)$ . Then the columns of  $[g^n]$  can be considered as points in  $\mathbb{P}^{k-1}(\mathbb{F}_q)$  of an orbit of  $\mathcal{T}$ . Conversely, we can obtain similarly a skew constacyclic code from an orbit of a projective map of  $\mathbb{P}^{k-1}(\mathbb{F}_q)$ .

Now, consider  $m$  orbits  $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_m$  of  $\mathcal{T}$  with large  $N$  and starting points  $P_i \in \mathcal{O}_i$  for  $i = 1, \dots, m$ . For simplicity, take  $P_1 \equiv P = (1, 0, \dots, 0)$  and define the matrix

$$[P_t, (P\tau)_t, \dots, (P\tau^{n_1-1})_t; (P_2)_t, (P_2\tau)_t, \dots, \dots, (P_2\tau^{n_2-1})_t; \dots; (P_m)_t, (P_m\tau)_t, \dots, (P_m\tau^{n_m-1})_t]$$

by  $[g^{n_1}] + P_2^{n_2} + \dots + P_m^{n_m}$ . Then, the matrix  $[g^N] + P_2^N + \dots + P_m^N$  generates a SQT code whose generator  $\mathbf{g}$  is given by the following result.

**Theorem 20.** *If  $P_i \in (\mathbb{F}_q^\theta)^k$  for  $i = 1, \dots, m$  are as above, then  $[g^N] + P_2^N + \dots + P_m^N$  generates a 1-generator Skew Quasi-Twisted (SQT)  $[mN, k]_q$ -code with generator*

$$\mathbf{g} = (h^*(x), b_2(x^{-1})h^*(x), \dots, b_m(x^{-1})h^*(x)) \in R^N,$$

where  $h^*(x)$  is as  $h(x)$  in Proposition 10 and  $b_i(x)$  is the polynomial given by  $(1, x, \dots, x^{k-1})P_i$  for  $2 \leq i \leq m$ .

*Proof.* Define  $H := [g^N] + P_2^N + \dots + P_m^N$  and note that

$$H = [P_t, (P\tau)_t, \dots, (P\tau^{N-1})_t; (P_2)_t, (P_2\tau)_t, \dots, \dots, (P_2\tau^{N-1})_t; \dots; (P_m)_t, (P_m\tau)_t, \dots, (P_m\tau^{N-1})_t]$$

with  $P_i \in (\mathbb{F}_q^\theta)^k$ ,  $\tau = \Theta \circ T_g$  and  $T_g \in GL(k, q)$  such that  $P\tau^N = \alpha P$ . By putting  $H_i := [(P_i)_t, (P_i\tau)_t, \dots, (P_i\tau^{N-1})_t]$  for all  $i = 1, \dots, m$ , we get  $H = [H_1 | H_2 | \dots | H_m]$ .

Take  $P_1 \equiv P := (1, 0, \dots, 0) = \vec{e}_1$  and note that  $P\tau^{j-1} = \vec{e}_j$  for all  $j = 1, \dots, k$ , where  $\vec{e}_j$  is the  $j$ -th canonical vector of  $\mathbb{F}_q^k$ . Then, for  $P_i \in (\mathbb{F}_q^\theta)^k$

and  $\lambda_{ij} \in \mathbb{F}_q^\theta$ , we have

$$P_i = \sum_{j=0}^{k-1} \lambda_{ij} P \tau^j = (P) \left( \sum_{j=0}^{k-1} \lambda_{ij} \tau^j \right) =: P \cdot P_i(\tau),$$

where  $P_i(x) := \sum_{j=0}^{k-1} \lambda_{ij} x^j$ . Thus

$$P_i \tau^h = \sum_{j=0}^{k-1} \lambda_{ij} P \tau^{j+h} = P \tau^h \cdot P_i(\tau), \quad \forall h = 0, \dots, N-1$$

and, for  $i = 1, \dots, m$ , this implies that

$$\begin{aligned} H_i &= [(P_i)_t, (P_i \tau)_t, \dots, (P_i \tau^{N-1})_t] \\ &= [(P \cdot P_i(\tau))_t, (P \tau \cdot P_i(\tau))_t, \dots, (P \tau^{N-1} \cdot P_i(\tau))_t] \\ &= P_i(\tau)_t \cdot [P_t, (P \tau)_t, \dots, (P \tau^{N-1})_t] \\ &= P_i(\tau)_t \cdot H_1 \end{aligned}$$

Let  $H_1^*$  be the generator matrix of  $\mathcal{C}^\perp$  with  $\mathcal{C} = \langle g(x) \rangle$  written as

$$H_1^* := \begin{pmatrix} h^*(x) \\ x h^*(x) \\ \vdots \\ x^{k-1} h^*(x) \end{pmatrix} = [J \mid \widehat{H}_1^*]$$

with  $\det(J) \neq 0$ , where  $h^*(x) = \theta^{N-k}(h_0)^{-1} x^{N-k} h(x^{-1})$  with  $x^N - \alpha = g(x)h(x)$ . By hypothesis,  $H_1$  is also a parity check matrix of  $\mathcal{C}$  which can be written as  $H_1 = [I_k \mid \widehat{H}_1]$ , where  $I_k$  is the identity matrix of dimension  $k$ . This implies that  $J^{-1} H_1^* = H_1$  and  $J^{-1} \widehat{H}_1^* = \widehat{H}_1$ .

Let  $A$  be a matrix with  $N$  columns and define the linear operator  $\diamond$  as follows:

$$x^{-1} \diamond A := A \cdot \left( \begin{array}{ccc|c} 0 & \cdots & 0 & \alpha \\ 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \end{array} \right).$$

Observe that  $x^{-1} \diamond (A' \cdot B') = A' \cdot (x^{-1} \diamond B')$  for any two matrices  $A'$  and  $B'$  such that  $A' \cdot B'$  is well defined and  $B'$  has  $N$  columns.

Furthermore, for  $h = 0, \dots, N-1$ , we get

$$\begin{aligned}
 x^{-1} \diamond H_1 &= x^{-1} \diamond [P_t, (P\tau)_t, \dots, (P\tau^{N-1})_t] \\
 &= [(P\tau)_t, \dots, (P\tau^{N-1})_t, \alpha P_t] \\
 &= [(P\tau)_t, \dots, (P\tau^{N-1})_t, (P\tau^N)_t] \\
 &= (\tau)_t \cdot H_1 \\
 x^{-2} \diamond H_1 &= x^{-1} \diamond (x^{-1} \diamond H_1) \\
 &= x^{-1}((\tau)_t \cdot H_1) \\
 &= (\tau^2)_t \cdot H_1 \\
 &\vdots \\
 x^{-h} \diamond H_1 &= (\tau^h)_t \cdot H_1
 \end{aligned}$$

Hence, we have

$$\begin{aligned}
 H_i &= P_i(\tau)_t \cdot H_1 = P_i(x^{-1}) \diamond (J^{-1} \cdot H_1^*) = J^{-1} \cdot (P_i(x^{-1}) \diamond H_1^*) = \\
 &= J^{-1} \cdot \left( P_i(x^{-1}) \diamond \begin{pmatrix} h^*(x) \\ xh^*(x) \\ \vdots \\ x^{k-1}h^*(x) \end{pmatrix} \right) = J^{-1} \cdot \begin{pmatrix} P_i(x^{-1}) \cdot h^*(x) \\ P_i(x^{-1}) \cdot xh^*(x) \\ \vdots \\ P_i(x^{-1}) \cdot x^{k-1}h^*(x) \end{pmatrix} \\
 &= J^{-1} \cdot \begin{pmatrix} P_i(x^{-1}) \cdot h^*(x) \\ x \cdot P_i(x^{-1})h^*(x) \\ \vdots \\ x^{k-1} \cdot P_i(x^{-1})h^*(x) \end{pmatrix} =: J^{-1} \cdot H_i^*
 \end{aligned}$$

Therefore, we conclude that

$$H = [H_1|H_2|\dots|H_m] = [J^{-1}H_1^*|J^{-1}H_2^*|\dots|J^{-1}H_m^*] = J^{-1}[H_1^*|H_2^*|\dots|H_m^*],$$

where  $\begin{pmatrix} P_i(x^{-1}) \cdot h^*(x) \\ x \cdot P_i(x^{-1})h^*(x) \\ \vdots \\ x^{k-1} \cdot P_i(x^{-1})h^*(x) \end{pmatrix}$ , i.e.  $[H_1|H_2|\dots|H_m]$  and  $[H_1^*|H_2^*|\dots|H_m^*]$  are two generator matrices of the same  $[mN, k]_q$ -code.  $\square$

The following MAGMA Program 5 defines the function `SQT(m,N,g)` which gives an application of the above result :

**Program 5.**

```

SQT:=function(m,N,g)
g1:=R!g; d:=Degree(g1); if d ge 1 then
TT:=R![0,1]; CM:=VerticalJoin(HorizontalJoin(ZeroMatrix(F,
d-1,1), ScalarMatrix(F,d-1,1)), Matrix(F,1,d,[-Eltseq(g1)[k]:
k in {1..d}])); PS<[x]>:=ProjectiveSpace(F,d-1);
PointsPS:={PS!p : p in Points(Scheme(PS,[0]))};
PointsPS2:=PointsPS; OrbN:={}; repeat
S:=Random(PointsPS2); PP:=Matrix(F,1,d,[S[k]: k in {1..d}]);
jj:=0; repeat
jj:=jj+1; PP:=Matrix(F,1,d,[SpecialEvaluate(TT,PP[1][i]):
i in {1..d}])*CM; PPP:=PS![PP[1][i]: i in {1..d}];
PointsPS2:=PointsPS2 diff {PPP}; until S eq PPP; if jj eq N then
OrbN:=OrbN join {S}; end if;
until PointsPS2 eq {}; P1:=HorizontalJoin(Matrix(F,1,1,[1]),
ZeroMatrix(F,1,d-1)); V1:=PS![P1[1][i]: i in {1..d}];
OrbN2:=OrbN diff {V1}; if #OrbN2 ge m then
S2:={}; for l in {1..m-1} do
RR:=Random(OrbN2 diff S2); S2:=S2 join {RR}; end for;
S1:={@ q : q in S2 @}; PCM1:=P1; PCM2:=P1;
for h in {1..N-1} do
PCM1:=Matrix(F,1,d,[SpecialEvaluate(TT,PCM1[1][i]): i in
{1..d}])*CM; PCM2:=VerticalJoin(PCM2,PCM1); end for;
PCM3:=Transpose(PCM2); for ii in {1..m-1} do
P:=Matrix(F,1,d,[S1[ii][j]: j in {1..d}]); PP:=P; PCM1:=P;
PCM2:=P; for h in {1..N-1} do
PCM1:=Matrix(F,1,d,[SpecialEvaluate(TT,PCM1[1][i]): i in
{1..d}])*CM; PCM2:=VerticalJoin(PCM2,PCM1); end for;
PCM3:=HorizontalJoin(PCM3, Transpose(PCM2)); end for;
LC:=LinearCode(PCM3); print
"===== "; print " ";
print "Skew Quasi Twisted Code of type: ",
N, N-d, MinimumWeight(LC); print "Polynomial generator:";
print g1; print " "; print "Companion Matrix:"; print CM;
print " "; print "Parity Check Matrix:"; print PCM3; print " ";
print "===== "; else
print "There are not enough orbits of length", N ;
end if; end if; return "end"; end function;

```

**Example 21.** Consider  $\mathbb{F}_8 = \{0, 1, w, w^2, \dots, w^6\}$ . From Program 2, by using the command `SD(7, w^3)` it follows that  $g(x) = x^4 - (w^3 + x + w^2 x^2) \in \mathbb{F}[x; \theta]$  divides  $x^7 - w^3$ , where  $\theta(x) = x^4$  for every  $x \in \mathbb{F}_8$ . Moreover, by Program 5 with the command `SQT(2, 7, [w^3, 1, w^2, 0, 1])` we see that the point  $P_2 := [0 : w^4 : 0 : 1] \in \mathbb{P}^3(\mathbb{F}_8)$  has an orbit of length 7. So, we get



a SQT  $[14, 4, 7]_8$ -code whose generator matrix is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & w^3 & 0 & 1 & 0 & w^3 & 0 & 0 & w^3 & w & 1 \\ 0 & 1 & 0 & 0 & 1 & w^5 & w^4 & w^4 & 1 & w^5 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & w^2 & 1 & 0 & 0 & 0 & 1 & w^6 & w^2 & 0 & w^6 \\ 0 & 0 & 0 & 1 & 0 & w & 1 & 1 & 0 & 0 & 1 & w^3 & w & 0 \end{pmatrix}.$$

For simplicity of notation, let us denote  $w, w^2, \dots, w^6$  with  $2, 3, \dots, 7$ , respectively. With this notation, the above parity-check matrix can be written simply as  $[g]^7 + P_2^7 = [4130]^7 + 0501^7$ .

**Example 22.** Consider  $\mathbb{F}_9 = \{0, 1, \beta, \beta^2, \dots, \beta^7\}$ , where  $\beta$  is a root of  $x^2 + 2x + 2 \in \mathbb{F}_3[x]$ . We denote  $0, 1, \beta, \beta^2, \dots, \beta^7$  by  $0, 1, 2, 3, \dots, 8$ , respectively. We set that  $g(x) = x^4 + (1 + 8x + 5x^2 + 4x^3) = x^4 - (5 + 4x + x^2 + 8x^3) \in \mathbb{F}_9[x; \theta]$  divides  $x^5 - 2$  with  $\theta(a) = a^3$  for every  $a \in \mathbb{F}_9$ . Let  $\mathcal{T}$  be the semi-linear map defined by  $\theta$  and  $g(x)$ . Consider the following three points  $P_1, P_2$  and  $P_3$  of  $\mathbb{P}^3(\mathbb{F}_9)$ :

$$P_1 = [1 : 0 : 0 : 0], P_2 = [1 : 6 : 8 : 1], P_3 = [4 : 7 : 4 : 1].$$

Then, under  $\mathcal{T}$ , the orbit of  $P_1$  is of length 5 and the orbits of  $P_2$  and  $P_3$  are both of length 10. Thus we deduce that

$$G = [4518]^5 + 1681^{10} + 4741^{10}$$

generate a SQT  $[25, 4, 19]_9$ -code. By comparing the distance of this code with that in the database of MAGMA, we can observe that it reaches the best known distance (BKLC) for a linear  $[25, 4]_9$ -code.

Finally, as an application of Theorem 20 and Program 5, Table 1 gives an example of how to construct some known linear codes with BKLC distance as SQT codes for small values of  $q$ .

## 2. A LOWER BOUND FOR THE DISTANCE

In [9] the author shows how a factorization of a skew polynomial can be made in a suitable commutative polynomial ring. By this method, we can transfer some properties of constacyclic codes to skew constacyclic codes and vice versa. In particular, a factorization of a skew polynomial in  $\mathbb{F}_q[x; \theta]$  can be made in  $\mathbb{F}_q[x]$  by a Leroy's algorithm (see Theorem 2.5, [9]). For any prime number  $p$  and an integer  $i \geq 1$ , he defines  $[i] := \frac{p^i - 1}{p - 1}$  and

$$\mathbb{F}_q[x^{\square}] := \left\{ \sum_{i=0}^m \alpha_i x^{[i]} \in \mathbb{F}_q[x] : m \in \mathbb{Z}_{\geq 0} \right\}.$$

Note that the Leroy's algorithm and the above definitions can be generalized by considering a power of the Frobenius automorphism. More precisely, let  $\mathbb{F}_q$  be a finite field with  $q = p^t$  and  $p$  prime, and consider the automorphism  $\theta(a) = a^{p^s}$  for all  $a \in \mathbb{F}_q$  with  $0 \leq s \leq t - 1$ .

$[n, k, d]_q$	Generator Matrix	$N$	$\alpha$	$\theta$
$[21, 6, 12]_4$	$[131313]^7 + 220211^{14}$	7	2	2
$[25, 4, 17]_4$	$[1313]^5 + 3331^{10} + 2310^{10}$	5	2	2
$[35, 6, 22]_4$	$[131313]^7 + 123210^{14} + 113110^{14}$	7	2	2
$[35, 4, 24]_4$	$[1212]^5 + 0321^{10} + 1031^{10} + 1301^{10}$	5	3	2
$[40, 4, 28]_4$	$[1313]^5 + 0321^{10} + 3301^{10} + 1301^{10} + 1010^5$	5	2	2
$[45, 4, 32]_4$	$[1212]^5 + 2100^{10} + 1311^{10} + 0101^{10} + 3321^{10}$	5	2	2
$[49, 6, 32]_4$	$[131313]^7 + 233101^{14} + 312221^{14} + 231310^{14}$	7	2	2
$[50, 4, 36]_4$	$[1212]^5 + 1231^{10} + 1101^{10} + 2231^{10} + 3321^{10} + 3100^5$	5	3	2
$[55, 4, 36]_4$	$[1313]^5 + 2011^{10} + 1131^{10} + 2221^{10} + 1331^{10} + 0310^5$	5	2	2
$[60, 4, 44]_4$	$[1313]^5 + 1110^{10} + 0231^{10} + 0031^{10} + 3111^{10} + 3311^{10} + 2021^5$	5	2	2
$[65, 4, 48]_4$	$[1212]^5 + 2201^{10} + 1011^{10} + 2131^{10} + 1310^{10} + 0211^{10} + 3100^5 + 3031^5$	5	3	2
$[85, 4, 64]_4$	$[1212]^5 + 3211^{10} + 0011^{10} + 3301^{10} + 1301^{10} + 1331^{10} + 3121^{10} + 1331^{10} + 1010^5 + 0210^5$	5	3	2
$[34, 3, 28]_8$	$[175]^4 + 721^{12} + 610^{12} + 111^6$	4	2	4
$[50, 4, 41]_8$	$[6156]^5 + 5331^{15} + 5610^{15} + 6321^{15}$	5	2	4
$[65, 5, 56]_8$	$[6156]^5 + 5541^{15} + 7310^{15} + 3110^{15} + 1531^{15}$	5	1	2
$[25, 4, 19]_9$	$[4518]^5 + 1681^{10} + 4741^{10}$	5	6	3
$[30, 4, 24]_9$	$[4518]^5 + 4801^{10} + 8771^{10} + 5810^5$	5	6	3
$[42, 4, 34]_9$	$[2030]^6 + 8121^{12} + 6821^{12} + 0531^{12}$	6	7	3

TABLE 1. Skew Quasi-Twisted Codes with BKLC distance.

By putting  $[i]_s := \frac{(p^s)^i - 1}{p^s - 1}$  instead of  $[i]$ , the polynomial ring  $\mathbb{F}_q[x^{\mathbb{N}}]$  can be replaced by

$$\mathbb{F}_q[x^{\mathbb{N}^s}] := \left\{ \sum_{i \geq 0} \alpha_i x^{[i]_s} \in \mathbb{F}_q[x] \ : \ m \in \mathbb{Z}_{\geq 0} \right\} \subseteq \mathbb{F}_q[x].$$

Finally, note that  $[i]_s = [i]$  and  $\mathbb{F}_q[x^{\mathbb{N}^s}] = \mathbb{F}_q[x^{\mathbb{N}}]$  for  $s = 1$ .

**Definition 23.** A  $[p^s]$ -code  $\mathcal{C}^{\square^s} \subseteq \mathbb{F}_q^{[n]_s}$  is a linear code generated by a  $[p^s]$ -polynomial in  $\mathbb{F}_q[x^{\square^s}]$ .

**Proposition 24.** Let  $\mathcal{C} \subseteq \mathbb{F}_q^n$  be a skew  $\alpha$ -cyclic code generated by  $f(t) \in \mathbb{F}_q[t; \theta]$  for some  $\alpha \in \mathbb{F}_q^*$ . Then the  $[p^s]$ -code  $\mathcal{C}^{\square^s} \subseteq \mathbb{F}_q^{[n]_s}$ , generated by the associated  $[p^s]$ -polynomial  $f^{\square^s}(t)$ , is an  $\alpha$ -cyclic code.

*Proof.* From Theorem 5, we know that  $f(t)$  is a right divisor of  $x^n - \alpha$ . Moreover, by Theorem 2.5 [9], we see that the associated  $[p^s]$ -polynomial  $f^{\square^s}(x) \in \mathbb{F}_q[x^{\square^s}]$  to  $f(t)$  is a right divisor of  $x^{[n]_s} - \alpha$ . Therefore the code  $\mathcal{C}^{\square^s} \subseteq \mathbb{F}_q^{[n]_s}$  is also an  $\alpha$ -cyclic code.  $\square$

**Remark 25.** More in general, if  $\mathcal{C} \subseteq \mathbb{F}_q^n$  is a skew  $\theta$ -module code generated by  $g(t) \in \mathbb{F}_q[t; \theta]$ , then by [9, Theorem 2.5] we see that the code  $\mathcal{C}^{\square^s} \subseteq \mathbb{F}_q^{[n]_s}$  is also a module code generated by  $g^{\square^s}(x) \in \mathbb{F}_q[x]$ .

**Theorem 26.** Let  $\mathcal{C} \subseteq \mathbb{F}_q^n$  be a linear code generated by  $f(t) \in \mathbb{F}_q[t; \theta]$  and let  $\mathcal{C}^{\square^s} \subseteq \mathbb{F}_q^{[n]_s}$  be the linear code generated by  $f^{\square^s}(x) \in \mathbb{F}_q[x^{\square^s}]$ . Then

$$d(\mathcal{C}^{\square^s}) \leq d(\mathcal{C})$$

and equality holds if and only if there exists a polynomial of minimal weight in  $\mathcal{C}^{\square^s}$  which belongs to  $\mathbb{F}_q[x^{\square^s}]$ .

*Proof.* Let  $w(t) \in \mathcal{C}$  be a polynomial of minimal weight. By Theorem 5 we have  $w(t) = a(t) \cdot f(t)$  for some  $a(x) \in \mathbb{F}_q[t; \theta]$ . Then by Theorem 2.5 [9] we get  $w^{\square^s}(x) = b(x) \cdot f^{\square^s}(x)$  for some  $b(x) \in \mathbb{F}_q[x]$ , i.e.  $w^{\square^s}(x) \in \mathcal{C}^{\square^s}$ . Hence  $d(\mathcal{C}^{\square^s}) \leq wt(w^{\square^s}(x)) = wt(w(t)) = d(\mathcal{C})$ . This proves the first part of the statement.

Suppose now that  $d(\mathcal{C}^{\square^s}) = d(\mathcal{C})$  and let  $v(t) \in \mathcal{C}$  be a polynomial such that  $wt(v(t)) = d(\mathcal{C})$ . Note that  $v(t) = q(t) \cdot f(t)$  for some  $q(t) \in \mathbb{F}_q[t; \theta]$ . Thus, by Leroy's algorithm we have  $v^{\square^s}(x) = g(x) \cdot f^{\square^s}(x)$  for some  $g(x) \in \mathbb{F}_q[x]$ , i.e.  $v^{\square^s}(x) \in \mathcal{C}^{\square^s}$ . Since  $d(\mathcal{C}^{\square^s}) = d(\mathcal{C}) = wt(v(t)) = wt(v^{\square^s}(x))$ , we conclude that  $v^{\square^s}(x) \in \mathbb{F}_q[x^{\square^s}]$  is a polynomial in  $\mathcal{C}^{\square^s}$  of minimal weight.

Finally, let  $w^{\square^s}(x) \in \mathbb{F}_q[x^{\square^s}]$  be a minimal weight polynomial in  $\mathcal{C}^{\square^s}$ . Then  $w^{\square^s}(x) = a(x) \cdot f^{\square^s}(x)$  for some  $a(x) \in \mathbb{F}_q[x]$ . This shows that  $w(t) = b(t) \cdot f(t)$ , i.e.  $w(t) \in \mathcal{C}$ . Therefore, we can conclude that

$$d(\mathcal{C}^{\square^s}) \leq d(\mathcal{C}) \leq wt(w(t)) = wt(w^{\square^s}(x)) = d(\mathcal{C}^{\square^s}),$$

that is,  $d(\mathcal{C}^{\square^s}) = d(\mathcal{C})$ .  $\square$

**Proposition 27.** A  $[p^s]$ -code  $\mathcal{C}^{\square^s} \subseteq \mathbb{F}_q^{[n]_s}$  with  $\dim(\mathcal{C}^{\square^s}) < [n]_s$  cannot be a MDS code.

*Proof.* Suppose there is a MDS code  $\mathcal{C}^{\square^s} \subset \mathbb{F}_q^{[n]_s}$ . Then

$$d(\mathcal{C}^{\square^s}) = [n]_s - \dim(\mathcal{C}^{\square^s}) + 1 = \deg(f^{\square^s}(x)) + 1 = [\deg(f(t))] + 1,$$

where  $f^{\llbracket s \rrbracket}(x)$  is the generator polynomial of  $\mathcal{C}^{\llbracket s \rrbracket}$ . Furthermore, by the Singleton Bound we have  $d(\mathcal{C}) \leq \deg(f(t)) + 1$ , where  $\mathcal{C}$  is the code generated by  $f(t)$ . Note that  $\deg(f(t)) \geq 1$  and  $[i]_s > i$  for all  $i \in \mathbb{Z}_{>0}$ . Thus by Theorem 26 we deduce that

$$[\deg(f(t))]_s + 1 = d(\mathcal{C}^{\llbracket s \rrbracket}) \leq d(\mathcal{C}) \leq \deg(f(t)) + 1,$$

i.e.  $[\deg(f(t))]_s \leq \deg(f(t))$ , but this gives a numerical contradiction. Thus the code  $\mathcal{C}^{\llbracket s \rrbracket}$  cannot be a MDS code.  $\square$

**Lemma 28.** *Let  $\mathbb{F}_{q^{[k]_s}}^* = \langle w \rangle$  and  $\mathbb{F}_{q^{[k]_s}} \subseteq \mathbb{F}_{q^{[n]_s}}$ . Then*

$$[n]_s \leq q^{[k]_s} - 1 \iff \text{rank} \left( V_{[n]_s}^{\text{Id}}(w, w^2, \dots, w^{[n]_s-1}) \right) = [n]_s.$$

*Proof.*

Let  $\mathcal{N} := \left( V_{[n]_s}^{\text{Id}}(w, w^2, \dots, w^{[n]_s-1}) \right) =$

$$= \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & \cdots & w^{[n]_s-1} \\ 1 & w^2 & (w^2)^2 & \cdots & (w^{[n]_s-1})^2 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & w^{[n]_s-1} & (w^2)^{[n]_s-1} & \cdots & (w^{[n]_s-1})^{[n]_s-1} \end{pmatrix}.$$

“ $\Rightarrow$ ” Suppose that  $\text{rank}(\mathcal{N}) \neq [n]_s$ . Then we have

$$(*) \quad \det(\mathcal{N}) := \prod_{0 \leq i < j \leq [n]_s-1} (w^j - w^i) = 0,$$

that is,  $w^{j-i} = 1$  for some  $i, j$  such that  $0 \leq i < j \leq [n]_s - 1$ . So the order of  $w$  must be less than or equal to  $[n]_s - 1$ . Thus we get  $[n]_s \leq q^{[k]_s} - 1 = \text{ord}(w) \leq [n]_s - 1$ , which is impossible. Hence  $\det(\mathcal{N}) \neq 0$ , i.e.  $\text{rank} \left( V_{[n]_s}^{\text{Id}}(w, w^2, \dots, w^{[n]_s-1}) \right) = [n]_s$ .

“ $\Leftarrow$ ” Note that  $\text{rank} \left( V_{[n]_s}^{\text{Id}}(w, w^2, \dots, w^{[n]_s-1}) \right) = [n]_s$  implies by  $(*)$  that  $w^{j-i} \neq 1$  for any  $i, j$  such that  $0 \leq i < j \leq [n]_s - 1$ . Thus  $q^{[k]_s} - 1 = \text{ord}(w) > [n]_s - 1$ , i.e.  $[n]_s \leq q^{[k]_s} - 1$ .  $\square$

Finally, let us give here an application of the above arguments to obtain a lower bound for the distance of a skew constacyclic code by finding roots of polynomials in  $\mathbb{F}_q[x]$  instead of  $\mathbb{F}_q[t; \theta]$ .

**Theorem 29.** *With the same notation as above, let  $\mathcal{C} \subseteq \mathbb{F}_q^n$  be a skew  $\theta$ -module code with generator polynomial  $g(t) \in \mathbb{F}_q[t; \theta]$  of degree  $k$ . If*

$$k \geq \log_{p^s} \left[ 1 + \left( \frac{p^s - 1}{r} \right) \cdot \log_p \left( \frac{(p^s)^n + p^s - 2}{p^s - 1} \right) \right]$$

and  $g^{\llbracket s \rrbracket}(\omega^{l+ci}) = 0$  for  $i = 0, \dots, \Delta - 2$ , some  $l \in \mathbb{Z}_{\geq 0}$  and  $c$  such that  $(c, q^{[k]_s} - 1) = 1$ , where  $\mathbb{F}_{q^{[k]_s}}^* = \langle \omega \rangle$ , then  $d(\mathcal{C}) \geq \Delta$ .

*Proof.* Note that

$$k \geq \log_{p^s} \left[ 1 + \left( \frac{p^s - 1}{r} \right) \cdot \log_p \left( \frac{(p^s)^n + p^s - 2}{p^s - 1} \right) \right] \iff$$

$$r \left( \frac{(p^s)^k - 1}{p^s - 1} \right) \geq \log_p (1 + [n]_s) \iff p^{r \cdot [k]_s} \geq (1 + [n]_s) \iff q^{[k]_s} - 1 \geq [n]_s .$$

Thus  $\text{ord}(\omega) = q^{[k]_s} - 1 \geq [n]_s$ . Furthermore, since  $(c, q^{[k]_s} - 1) = 1$ , we have

$$\mathcal{N}_j^{\text{id}}(\omega^c) = (\omega^c)^j \neq 1, \text{ for } j = 1, \dots, [n]_s - 1.$$

From Remark 25 we know that  $\mathcal{C}^{\square_s} \subseteq \mathbb{F}_q^{[n]_s}$  is a  $\theta$ -module code with generator polynomial  $g^{\square_s}(x) \in \mathbb{F}_q[x]$ ,  $\mathbb{F}_{q^{[k]_s}}^* = \langle \omega \rangle$  with  $\omega \in \mathbb{F}_{q^{[k]_s}}$  and by hypothesis  $g^{\square_s}(\omega^{l+ci}) = 0$ , for  $i = 0, \dots, \Delta - 2$  and some  $l \in \mathbb{Z}_{\geq 0}$ . Then by Theorem 26 and [11, Theorem 3.9] we conclude that  $d(\mathcal{C}) \geq d(\mathcal{C}^{\square_s}) \geq \Delta$ .  $\square$

### 3. CONCLUSION

In this work, we consider skew constacyclic codes and some of the main algebraic and geometric properties of their dual codes. First of all, we prove again in an easy and direct way that the dual code of a skew  $\alpha$ -cyclic code is a skew  $\alpha^{-1}$ -cyclic code and we show explicitly how to build its generator polynomial. Secondly, we observe that the parity check matrix of a skew  $\alpha$ -cyclic code has a very special form because its columns are related to orbits of points in projective spaces via semi-linear maps. Moreover, a generalization to the non-commutative case of a result on 1-generator Quasi Twisted (QT) codes is given and by a commutative method due to A. Leroy we prove two lower bounds for the distance of skew  $\theta$ -module codes, in particular for skew constacyclic codes. Finally, from a computer point of view, some MAGMA programs are given as application of the main theoretical results and by them a table is constructed, where for small fields some examples of known linear codes with BKLC distance are constructed as 1-generator skew QT codes.

### REFERENCES

- [1] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.
- [2] D. Boucher, W. Geiselmann and F. Ulmer, *Skew-cyclic codes*, Appl. Algebra Engrg. Comm. Comput. **18** (2007), no. 4, 379–389.
- [3] D. Boucher and F. Ulmer, *Codes as modules over skew polynomial rings*, Cryptography and coding, Lecture Notes in Comput. Sci. **5921**, Springer, Berlin, 2009, 38–55.
- [4] D. Boucher and F. Ulmer, *A note on the dual codes of module skew codes*, Cryptography and coding, Lecture Notes in Comput. Sci. **7089**, Springer, Heidelberg, 2011, 230–243.
- [5] D. Boucher and F. Ulmer, *Self-dual skew codes and factorization of skew polynomials*, J. Symbolic Comput. **60** (2014), 47–61.

- [6] N. Fogarty and H. Gluesing-Luerssen, *A circulant approach to skew-constacyclic codes*, Finite Fields Appl. **35** (2015), 92–114.
- [7] T. Maruta, *A geometric approach to semi-cyclic codes*, Advances in finite geometries and designs (Chelwood Gate, 1990), Oxford Sci. Publ., Oxford Univ. Press, New York (1991), 311–318.
- [8] T. Maruta, M. Shinohara and M. Takenaka, *Constructing linear codes from some orbits of projectivities*, Discrete Math. **308** (2008), no. 5–6 , 832–841.
- [9] A. Leroy, *Noncommutative polynomial maps*, J. Algebra Appl. **11** (2012), no. 4, 1250076, 16 pp.
- [10] L.F. Tapia Cuitiño and A.L. Tironi, *Dual codes of product semi-linear codes*, Linear Algebra Appl. **457** (2014), 114–153.
- [11] L.F. Tapia Cuitiño and A.L. Tironi, *Some properties of skew codes over finite fields*, (2015), arXiv:1507.02726.

DEPARTAMENTO DE MATEMÁTICA, UNIVERSIDAD DE CONCEPCIÓN, CASILLA 160-C,  
CONCEPCIÓN, CHILE

*E-mail address:* alexisalmendras@udec.cl, atironi@udec.cl